Upper Bound on Error Exponent of Regular LDPC Codes Transmitted over the BEC

Idan Goldenberg   David Burshtein
School of Electrical Engineering
Tel-Aviv University
Tel-Aviv 69978, Israel
E-mail: {idang,burstyn}@eng.tau.ac.il

Abstract

The error performance of the ensemble of typical LDPC codes transmitted over the binary erasure channel (BEC) is analyzed. In the past, lower bounds on the error exponents were derived. In this paper a probabilistic upper bound on this error exponent is derived. This bound holds with some confidence level.

Index Terms: Block codes, error exponent, expurgated ensemble, stopping sets, low-density parity-check (LDPC) codes, iterative decoding, binary erasure channel (BEC).

I. INTRODUCTION

Low-density parity-check (LDPC) codes, discovered by Gallager [1], have been widely researched over the last decade and a half. Asymptotic results are widely known for these codes, including results on the performance under maximum-likelihood (ML) decoding [1], [2], [3], [4], [5], average ensemble distance spectra [1], [6], [7], [8], [9], stopping set distributions [7], [8], [9], [10], thresholds for iterative decoding using density evolution [11], [12], and others. However, accurate finite-length analysis of LDPC codes under iterative sum-product decoding is currently available only for the binary erasure channel (BEC) [13]. This is due to the simplicity of the channel model and the graph-based iterative decoder which lends itself to a more detailed analysis. Analysis of the combinatorial properties of stopping sets and their contribution to the error performance reveals that the average error performance of the LDPC ensemble is proportional to the inverse of a polynomial in the block length N [7]. This behavior is attributed to the existence of "bad" codes which possess small stopping sets, and otherwise would decrease *exponentially* with N if these codes were removed from the ensemble. Fortunately, these "bad" codes constitute a small fraction of the entire ensemble whose size is proportional to the inverse of a polynomial in N.

After removing the undesirable codes, we obtain an *expurgated ensemble*, for which there exists a positive error exponent. In [7], lower bounds on this error exponent of typical codes in the regular and irregular LDPC code ensembles were derived. In this paper we obtain an upper bound on this exponent, and compare it with the above mentioned lower bounds. Similar to [5], which considers upper bounds on the error exponent of LDPC codes under ML decoding, our bounds depend on some confidence level.

The correspondence is organized as follows. Section II introduces notation and preliminary material.

Section III introduces a lower bound on the error (erasure) probability from which an upper bound on the exponent is derived. Section IV introduces numerical results and comparisons with previous results. Section V concludes the paper.

II. PRELIMINARIES

A. Notation

We will use the following notation throughout the paper.

- Let $\{\alpha_l\}_{l=1}^k$ be a set of non-negative real numbers, such that $\sum_l \alpha_l \leq 1$. The entropy function of $\{\alpha_l\}_{l=1}^k$ is defined as

$$h(\alpha_1, \ldots, \alpha_k) = -\sum_{l=1}^k \alpha_l \log(\alpha_l) - \left(1 - \sum_{l=1}^k \alpha_l\right) \log\left(1 - \sum_{l=1}^k \alpha_l\right)$$

where $\log$ is the base-2 logarithm. We use the convention $0 \log 0 = 0$.

- Given an integer n and integers $(n_1, \ldots, n_k)$ such that $\sum_l n_l \leq n$,

$$\binom{n}{n_1, n_2, \ldots, n_k} \triangleq \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot \left(n - \sum_{l=1}^k n_l\right)!}$$

is the multinomial coefficient of n over $(n_1, \ldots, n_k)$. We will use the following property of multinomial coefficients

$$\log\binom{n}{n_1, n_2, \ldots, n_k} = n\left(h\left(\frac{n_1}{n}, \ldots, \frac{n_k}{n}\right) + o(1)\right) \tag{1}$$

which is easily proven using Stirling's approximation.

- If $p(x)$ is a polynomial, then we will denote the coefficient of x^i by $[x^i] p(x)$, i.e,

$$p(x) = \sum_i [x^i] p(x) x^i$$

The same notation is extended for use with multivariate polynomials, e.g.,

$$p(x, y, z) = \sum_{i,j,k} [x^i y^j z^k] p(x, y, z) x^i y^j z^k$$

B. A Second-Order Inequality for Probabilities

Dawson and Sankoff [14] obtained a lower bound on the probability of a finite union of events. Their result asserts the following. Let $\{A_i\}_{i=1}^M$ be a finite family of events in a probability space (Ω, P). Denote

$$\tilde{S}_1 = \sum_{i \in I} \Pr(A_i) \qquad \tilde{S}_2 = \sum_{\substack{i,j \in I \\ i > j}} \Pr(A_i \cap A_j)$$

where $I = \{1, \ldots, M\}$. Then

$$\Pr\left(\bigcup_{i \in I} A_i\right) \geq \frac{2}{r+1}\tilde{S}_1 - \frac{2}{r(r+1)}\tilde{S}_2 \tag{2}$$

for any $r \in \{1, \ldots, M - 1\}$.

Following the derivation in [14], we derive a result which generalizes (2). For a probability event A, denote by $\mathbf{1}_{\{A\}}$ to be the indicator (random variable) over A, i.e, for $\omega \in \Omega$,

$$\mathbf{1}_{\{A\}}(\omega) = \begin{cases} 1 & \omega \in A \\ 0 & \omega \notin A \end{cases}$$

Our result asserts that for all $\omega \in \Omega$,

$$\mathbf{1}_{\{\cup_{i=1}^{M} A_i\}} \geq \frac{2}{r+1} S_1 - \frac{2}{r(r+1)} S_2 \tag{3}$$

where

$$S_1 = \sum_{i \in I} \mathbf{1}_{\{A_i\}} \qquad S_2 = \sum_{\substack{i,j \in I \\ i > j}} \mathbf{1}_{\{A_i\}} \mathbf{1}_{\{A_j\}}$$

By taking the expectation over both sides of (3), we get (2) as a special case. We prove (3) in Appendix I.

C. LDPC Code Ensembles

We consider the standard bipartite graph-based (c, d)-regular LDPC code ensemble with block length N and design rate R. In this ensemble a randomly chosen permutation is used to match the cN left sockets to the $d(1 - R)N$ right sockets. The actual rate of the code is at least $R \triangleq 1 - c/d$.

III. UPPER BOUND ON ERROR EXPONENT FOR THE BEC

Recall that a *stopping set* $\mathcal{S}$ of a bipartite graph representation of an LDPC code is a set of variable nodes, such that each check node neighbor of $\mathcal{S}$ is connected to $\mathcal{S}$ by at least two edges. As explained in [13], iterative decoding of LDPC codes succeeds if and only if the set of variable nodes which correspond to erasures does not contain a subset which is a stopping set.

The *expurgated* (c, d)-regular LDPC ensemble $\mathcal{C}^\gamma$ is derived from the (c, d)-regular ensemble $\mathcal{C}^0$ by removing all the codes containing stopping sets of size γN or less. It was shown in [7] that for ensembles with $c > 2$, if γ is selected below a certain threshold α_0, then almost all codes in $\mathcal{C}^0$ belong to $\mathcal{C}^\gamma$. In other words, if $\mathcal{C}$ is drawn at random from $\mathcal{C}^0$

$$\Pr\left(\mathcal{C} \in \mathcal{C}^\gamma\right) = 1 - o(1) \quad \forall \gamma < \alpha_0 \tag{4}$$

The number $\alpha_0 N$ may therefore be considered to be the typical minimum stopping set size of $\mathcal{C}^0$. Since the behavior of $\mathcal{C}^0$ is dominated by a small fraction of "bad" codes, we will be interested in the performance of codes drawn at random from $\mathcal{C}^\gamma$. Let $\mathcal{C}$ be such a code.

Consider a BEC with erasure probability δ; the probability of unsuccessful decoding of any codeword from $\mathcal{C}$, $P_e^{\mathcal{C}}$ is given by

$$P_e^{\mathcal{C}} = \sum_{l=\gamma N}^{N} \delta^l (1-\delta)^{N-l} \sum_m \mathbf{1}_{\left\{\cup_{i=1}^{2^l-1} A_i^m\right\}} \tag{5}$$

where the index m runs over all sets of variable nodes containing exactly l nodes; for a particular set $\mathcal{S}_m$ of l variable nodes, $\{A_i^m\}$ is the event that the i'th (non-empty) subset of $\mathcal{S}_m$ (where $i = 1, \ldots, 2^l - 1$) is a stopping set. Note that every set of $N(1-R)+1$ variable nodes contains the support of a nonzero codeword[1]. Hence (since every codeword is a stopping set), every set of $N(1-R)+1$ variable nodes contains a stopping set. Therefore, the indicator appearing in the RHS of (5) may be replaced by 1 for $l > N(1-R)$, which yields

$$P_e^{\mathcal{C}} = \sum_{l=\gamma N}^{N(1-R)} \delta^l (1-\delta)^{N-l} \sum_m \mathbf{1}_{\left\{\cup_{i=1}^{2^l-1} A_i^m\right\}} + \sum_{l=N(1-R)+1}^{N} \binom{N}{l} \delta^l (1-\delta)^{N-l} \tag{6}$$

Next, we use (3) to lower-bound the indicator function in (6), giving

$$\mathbf{1}_{\left\{\cup_{i=1}^{2^l-1} A_i^m\right\}} \geq \frac{2}{r_l+1} S_1 - \frac{2}{r_l(r_l+1)} S_2 \tag{7}$$

where r is allowed to depend on the size of the set, and

$$S_1 = \sum_{i=1}^{2^l-1} \mathbf{1}_{\{A_i^m\}} \qquad S_2 = \sum_{i=1}^{2^l-1} \sum_{k=1}^{i-1} \mathbf{1}_{\{A_i^m\}} \mathbf{1}_{\{A_k^m\}} \tag{8}$$

Consider a stopping set $\mathcal{S}$ containing k variable nodes, where $k \leq l$. The number of sets of variable nodes of size l containing $\mathcal{S}$ as a subset is $\binom{N-k}{l-k}$. Hence, again letting m run over all subsets of size l, we have

$$\sum_m \sum_{i=1}^{2^l-1} \mathbf{1}_{\{A_i^m\}} = \sum_{k=1}^{l} \binom{N-k}{l-k} S_k^{\mathcal{C}} = \sum_{k=\gamma N}^{l} \binom{N-k}{l-k} S_k^{\mathcal{C}} \tag{9}$$

where $S_k^{\mathcal{C}}$ is the number of stopping sets with k variable nodes in $\mathcal{C}$; note that since $\mathcal{C}$ belongs to the expurgated ensemble, we have $S_k^{\mathcal{C}} = 0$ for $k < \gamma N$.

In a similar fashion we obtain

$$\sum_m \sum_{i=1}^{2^l-1} \sum_{j=1}^{i-1} \mathbf{1}_{\{A_i^m\}} \mathbf{1}_{\{A_j^m\}} = \sum_{\substack{\gamma N \leq j \leq i \leq l \\ 0 \leq k \leq j+\min(i-j-1,0) \\ i+j-k \leq l}} \binom{N-(i+j-k)}{l-(i+j-k)} S_{i,j,k}^{\mathcal{C}} \tag{10}$$

where $S_{i,j,k}^{\mathcal{C}}$ is the number of *pairs* of stopping sets, $(\mathcal{S}_1, \mathcal{S}_2)$ satisfying $|\mathcal{S}_1| = i$, $|\mathcal{S}_2| = j$, and $|\mathcal{S}_1 \cap \mathcal{S}_2| = k$. Recalling that both $\mathcal{S}_1$ and $\mathcal{S}_2$ must be subsets of a particular set of size l, their union must also be a subset, and therefore $|\mathcal{S}_1 \cup \mathcal{S}_2| = i+j-k \leq l$. Furthermore, the application of (3) requires summing over pairs of *distinct* events. Consequently, we cannot have $\mathcal{S}_1 = \mathcal{S}_2$, i.e., when $i = j$, we must have $k < j$;

---

[1]This is tantamount to saying that $N(1-R)+1$ columns in the parity check matrix, regardless of how they are chosen, are linearly dependent; this follows since the matrix has $N(1-R)$ rows.

this requirement is subsumed by imposing $0 \leq k \leq j + \min(i - j - 1, 0)$ in (10). Plugging (7)-(10) into (6), we get

$$
\begin{aligned}
P_e^{\mathcal{C}} &\geq \sum_{l=\gamma N}^{N(1-R)} \delta^l (1-\delta)^{N-l} \left[\frac{2}{r_l + 1} \sum_{i'=\gamma N}^{l} \binom{N - i'}{l - i'} S_{i'}^{\mathcal{C}} \right. \\
&\quad \left. - \frac{2}{r_l(r_l + 1)} \sum_{\substack{\gamma N \leq j \leq i \leq l \\ 0 \leq k \leq j + \min(i-j-1,0) \\ i+j-k \leq l}} \binom{N - (i + j - k)}{l - (i + j - k)} S_{i,j,k}^{\mathcal{C}} \right] + \sum_{l=N(1-R)+1}^{N} \binom{N}{l} \delta^l (1-\delta)^{N-l} \\
&\geq \sum_{l=\gamma N}^{N(1-R)} \left\{ \delta^{N\epsilon}(1-\delta)^{N(1-\epsilon)} \left[\frac{2}{r_l + 1} \max_{\gamma \leq \eta \leq \epsilon} \binom{N(1 - \eta)}{N(\epsilon - \eta)} S_{\eta N}^{\mathcal{C}} \right. \right. \\
&\quad \left. \left. - \frac{2}{r_l(r_l + 1)} (\epsilon N)^3 \max_{\substack{\gamma \leq \eta_2 \leq \eta_1 \leq \epsilon \\ 0 \leq \beta \leq \eta_2 \\ \eta_1 + \eta_2 - \beta \leq \epsilon}} \binom{N(1 - (\eta_1 + \eta_2 - \beta))}{N(\epsilon - (\eta_1 + \eta_2 - \beta))} S_{\eta_1 N, \eta_2 N, \beta N}^{\mathcal{C}} \right] \right\} \\
&\quad + \max_{1-R \leq \epsilon \leq 1} \left\{ \binom{N}{N\epsilon} \delta^{N\epsilon}(1-\delta)^{N(1-\epsilon)} \right\} \\
&\overset{(a)}{\geq} \max_{\gamma \leq \epsilon \leq 1-R} \left\{ \delta^{N\epsilon}(1-\delta)^{N(1-\epsilon)} \hat{P}_e^{\mathcal{C}}(\epsilon, N) \right\} + \max_{1-R \leq \epsilon \leq 1} \left\{ \binom{N}{N\epsilon} \delta^{N\epsilon}(1-\delta)^{N(1-\epsilon)} \right\}
\end{aligned}
$$

where

$$
\hat{P}_e^{\mathcal{C}}(\epsilon, N) \triangleq \left[\frac{2}{r_{\epsilon N} + 1} \max_{\gamma \leq \eta \leq \epsilon} \binom{N(1 - \eta)}{N(\epsilon - \eta)} S_{\eta N}^{\mathcal{C}} \right.
$$
$$
\left. - \frac{2}{r_{\epsilon N}(r_{\epsilon N} + 1)} (\epsilon N)^3 \max_{\substack{\gamma \leq \eta_2 \leq \eta_1 \leq \epsilon \\ 0 \leq \beta \leq \eta_2 \\ \eta_1 + \eta_2 - \beta \leq \epsilon}} \binom{N(1 - (\eta_1 + \eta_2 - \beta))}{N(\epsilon - (\eta_1 + \eta_2 - \beta))} S_{\eta_1 N, \eta_2 N, \beta N}^{\mathcal{C}} \right] \tag{11}
$$

and $\epsilon \triangleq \frac{l}{N}$, $\eta \triangleq \frac{i'}{N}$, $\eta_1 \triangleq \frac{i}{N}$, $\eta_2 \triangleq \frac{j}{N}$, and $\beta \triangleq \frac{k}{N}$; a sufficient condition in order for (a) to hold is that $\hat{P}_e^{\mathcal{C}}(\epsilon, N)$ be non-negative for $\gamma \leq \epsilon \leq 1 - R$. Later we will choose the value of $r_{\epsilon N}$ so that this condition is fulfilled.

By expressing the bound in exponential form, we get the following upper bound on the error exponent

$$
-\frac{1}{N} \log P_e^{\mathcal{C}} \leq - \max_{\gamma \leq \epsilon \leq 1} \left\{ \epsilon \log \delta + (1 - \epsilon) \log(1 - \delta) + \left\{ \begin{array}{ll} \frac{1}{N} \log P_e^{\mathcal{C}}(\epsilon, N) & \gamma \leq \epsilon \leq 1 - R \\ h(\epsilon) & 1 - R \leq \epsilon \leq 1 \end{array} \right\} \right\} + o(1)
$$

where we rely upon (1), and

$$
P_e^{\mathcal{C}}(\epsilon, N) \triangleq \frac{2}{r_{\epsilon N} + 1} 2^{-N E_1'} - \frac{2}{r_{\epsilon N}(r_{\epsilon N} + 1)} 2^{-N E_2'} \tag{12}
$$

$$
E_1' = - \max_{\gamma \leq \eta \leq \epsilon} \left\{ (1 - \eta) h\left(\frac{\epsilon - \eta}{1 - \eta} \right) + \frac{1}{N} \log S_{\eta N}^{\mathcal{C}} \right\} \tag{13}
$$

$$
E_2' = - \max_{\substack{\gamma \leq \eta_2 \leq \eta_1 \leq \epsilon \\ 0 \leq \beta \leq \eta_2 \\ \eta_1 + \eta_2 - \beta \leq \epsilon}} \left\{ (1 - (\eta_1 + \eta_2 - \beta)) h\left(\frac{\epsilon - (\eta_1 + \eta_2 - \beta)}{1 - (\eta_1 + \eta_2 - \beta)} \right) + \frac{1}{N} \log S_{\eta_1 N, \eta_2 N, \beta N}^{\mathcal{C}} \right\} \tag{14}
$$

Let $\mathcal{C}'$ be a randomly selected code from $\mathcal{C}^0$, and let $\overline{S}_i$ and $\overline{S}_{i,j,k}$ be the averages, over $\mathcal{C}^0$, of $S_i^{\mathcal{C}'}$ and $S_{i,j,k}^{\mathcal{C}'}$, respectively. We evaluate these average quantities and then relate them to $S_i^{\mathcal{C}}$ and $S_{i,j,k}^{\mathcal{C}}$[2]. In order to evaluate these quantities, we introduce the following notation.

$$\psi_i(x;d) \;=\; \sum_{l=i}^{d} \binom{d}{l} x^l = (1+x)^d - \sum_{l=0}^{i-1} \binom{d}{l} x^l \tag{15}$$

$$\Psi_{i_-,k_-,j_-}^{i_+,k_+,j_+}(x,y,z,d) \;=\; \sum_{\substack{i_-\leq i\leq i_+ \\ j_-\leq j\leq j_+ \\ k_-\leq k\leq k_+ \\ i+j+k\leq d}} \binom{d}{i,j,k} x^i y^j z^k \tag{16}$$

The average quantities satisfy

$$\overline{S}_i \;=\; \binom{N}{i} P_{s,1}(i) \tag{17}$$

$$\overline{S}_{i,j,k} \;=\; \binom{N}{i-k,k,j-k} P_{s,2}(i,j,k) \tag{18}$$

where $P_{s,1}(i)$ is the probability that a specific set of variable nodes, $\mathcal{S}$, is a stopping set, and $P_{s,2}(i,j,k)$ is the probability that a specific pair of sets - $\mathcal{S}_1$ containing i variable nodes and $\mathcal{S}_2$ containing j variable nodes, with $|\mathcal{S}_1 \cap \mathcal{S}_2| = k$, are both stopping sets.

To evaluate $P_{s,1}(i)$, we need to fix a set $\mathcal{S}$ of i variable nodes and count the number of possibilities of connecting their ic variable sockets to ic check sockets such that each of the L check nodes is either (a) not connected to any of the ic variable sockets, or (b) connected by at least two check sockets. This combinatorial problem can be solved by means of the enumeration function in (15). The total number of ways to connect ic variable sockets to Nc check sockets is $\binom{Nc}{ic}$, therefore

$$P_{s,1}(i) = \frac{\left[x^{ic}\right] \left(1 + \psi_2(x,d)\right)^L}{\binom{Nc}{ic}}$$

We proceed with the evaluation of $P_{s,2}(i,j,k)$. Given two sets $\mathcal{S}_1$ and $\mathcal{S}_2$ of variable nodes with $|\mathcal{S}_1| = i$, $|\mathcal{S}_2| = j$, $|\mathcal{S}_1 \cap \mathcal{S}_2| = k$, we need to count the number of possibilities of connecting $(i-k)c$ sockets from $\mathcal{S}_1/\mathcal{S}_2$, kc sockets from $\mathcal{S}_1 \cap \mathcal{S}_2$ and $(j-k)c$ sockets from $\mathcal{S}_2/\mathcal{S}_1$ to $(i+j-k)c$ check sockets, such that both $\mathcal{S}_1$ and $\mathcal{S}_2$ are stopping sets. This situation is depicted in Figure 1. Consider a check node α in the graph. From the definition of a stopping set, it can be seen that in order to have both $\mathcal{S}_1$ and $\mathcal{S}_2$ as stopping sets, α has to fall into one of the following disjoint categories:

- α is not connected at all to nodes in $\mathcal{S}_1 \cup \mathcal{S}_2$.
- α is connected by at least two edges to nodes in $\mathcal{S}_1/\mathcal{S}_2$ and is not connected to nodes in $\mathcal{S}_2$.
- α is connected by at least two edges to nodes in $\mathcal{S}_2/\mathcal{S}_1$ and is not connected to nodes in $\mathcal{S}_1$.
- α is connected by at least two edges to nodes in $\mathcal{S}_1/\mathcal{S}_2$ and by at least two edges to nodes in $\mathcal{S}_2/\mathcal{S}_1$, but is not connected to any node in $\mathcal{S}_1 \cap \mathcal{S}_2$.

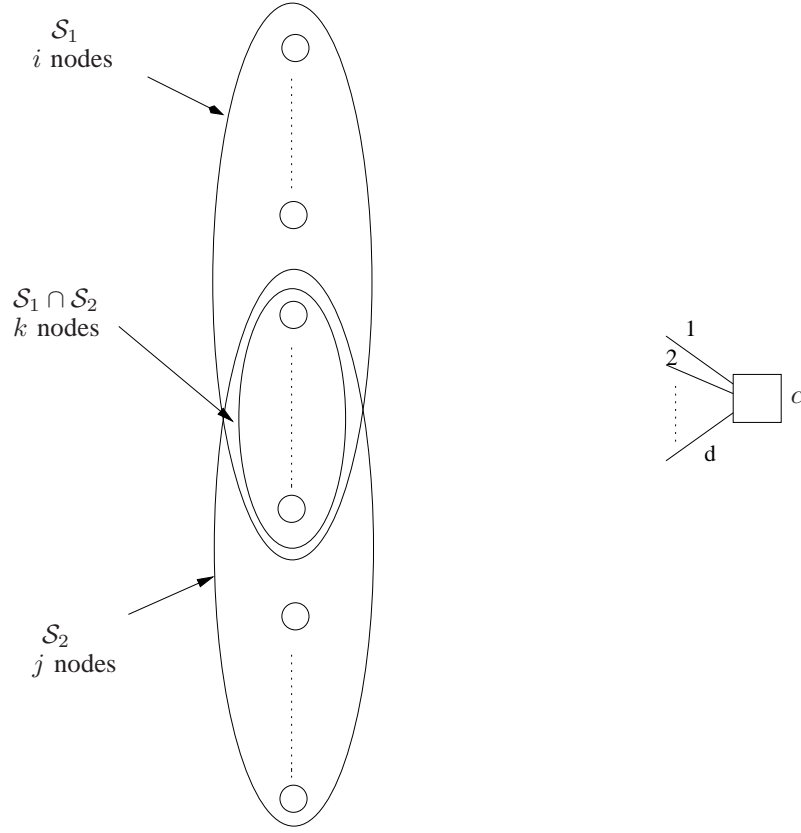[2]recall that in our context $\mathcal{C}$ is selected uniformly from $\mathcal{C}^\gamma$

Fig. 1.   Two intersecting stopping sets and a check node α

- α is connected by exactly one edge to a node in $\mathcal{S}_1 \cap \mathcal{S}_2$, and by at least one edge to nodes in $\mathcal{S}_1/\mathcal{S}_2$ and in $\mathcal{S}_2/\mathcal{S}_1$.
- α is connected by at least two edges to nodes in $\mathcal{S}_1 \cap \mathcal{S}_2$.

This combinatorial problem can be solved using the enumeration function given in (16). The total number of possibilities of connecting $(i-k)c$ sockets from $\mathcal{S}_1/\mathcal{S}_2$, kc sockets from $\mathcal{S}_1 \cap \mathcal{S}_2$ and $(j-k)c$ sockets from $\mathcal{S}_2/\mathcal{S}_1$ to Nc check sockets is $\binom{Nc}{(i-k)c, kc, (j-k)c}$. Therefore,

$$
\begin{aligned}
P_{s,2}(i,j,k) &= \left[x^{(i-k)c} y^{kc} z^{(j-k)c} \right] B(x,y,z,d)^L \cdot \binom{Nc}{(i-k)c, kc, (j-k)c}^{-1} \\
B(x,y,z,d) &\triangleq 1 + \Psi_{2,0,0}^{d,0,0}(x,y,z,d) + \Psi_{0,0,2}^{0,0,d}(x,y,z,d) + \Psi_{2,0,2}^{d-2,0,d-2}(x,y,z,d) \\
&\quad + \Psi_{1,1,1}^{d-1,1,d-1}(x,y,z,d) + \Psi_{0,2,0}^{d,d,d}(x,y,z,d)
\end{aligned}
\tag{19}
$$

We turn our attention back to the relation between the average quantities $\overline{S}_i$ and $\overline{S}_{i,j,k}$ and those of the randomly selected code, $S_i^{\mathcal{C}}$ and $S_{i,j,k}^{\mathcal{C}}$. By assuming that $\mathcal{C}$ is selected at random with uniform probability

from $\mathcal{C}^0$ and using conditioning, we have

$$\Pr\left(S_{i,j,k}^{\mathcal{C}} > N\overline{S}_{i,j,k} \mid \mathcal{C} \in \mathcal{C}^\gamma\right) \;=\; \frac{\Pr\left(S_{i,j,k}^{\mathcal{C}} > N\overline{S}_{i,j,k}\right) - \Pr\left(\mathcal{C} \notin \mathcal{C}^\gamma, S_{i,j,k}^{\mathcal{C}} > N\overline{S}_{i,j,k}\right)}{\Pr\left(\mathcal{C} \in \mathcal{C}^\gamma\right)}$$

$$\overset{(a)}{\leq} \frac{\Pr\left(S_{i,j,k}^{\mathcal{C}} > N\overline{S}_{i,j,k}\right)}{1 - o(1)} \overset{(b)}{\leq} \frac{1}{N(1 - o(1))} \tag{20}$$

where (a) is obtained using (4) and by omitting the negative term, and (b) is due to Markov's inequality. We conclude from (20) that w.p. (with probability) $1 - o(1)$, for $\mathcal{C}$ chosen randomly with uniform probability from $\mathcal{C}^\gamma$,

$$\frac{1}{N}\log S_{i,j,k}^{\mathcal{C}} \leq \frac{1}{N}\log \overline{S}_{i,j,k} + o(1) \tag{21}$$

By using conditioning once more we obtain

$$\Pr\left(1 - \epsilon \leq \frac{S_i^{\mathcal{C}}}{\overline{S}_i} \leq 1 + \epsilon \,\Big|\, \mathcal{C} \in \mathcal{C}^\gamma\right) \;\geq\; \frac{\Pr\left(1 - \epsilon \leq \frac{S_i^{\mathcal{C}}}{\overline{S}_i} \leq 1 + \epsilon\right) - \Pr\left(\mathcal{C} \notin \mathcal{C}^\gamma\right)}{\Pr\left(\mathcal{C} \in \mathcal{C}^\gamma\right)}$$

$$\overset{(a)}{\geq} \Pr\left(1 - \epsilon \leq \frac{S_i^{\mathcal{C}}}{\overline{S}_i} \leq 1 + \epsilon\right) + o(1) \tag{22}$$

where (a) is obtained by using (4) and replacing the denominator by 1.

Rathi [8] has obtained a concentration result on the stopping set distribution. His result implies the following. For any $\epsilon > 0$,

$$\Pr\left(1 - \epsilon \leq \frac{S_{\eta N}^{\mathcal{C}}}{\overline{S}_{\eta N}} \leq 1 + \epsilon\right) \geq 1 - \frac{\beta_{\eta,d,c}}{\epsilon^2} + o(1) \tag{23}$$

where $\beta_{\eta,d,c}$ is a constant given in Eq. (37) in Appendix II, independent of N, which satisfies $\beta_{\eta,d,c} \to 0$ when $d \to \infty$ and $\frac{c}{d}$ is kept constant. By setting $\epsilon \to 1$ in (23) and using (22), we conclude that w.p. at least $1 - \frac{\beta_{\eta,d,c}}{\epsilon^2} + o(1)$, for $\mathcal{C}$ chosen randomly with uniform probability from $\mathcal{C}^\gamma$,

$$\frac{1}{N}\log S_{\eta N}^{\mathcal{C}} \geq \frac{1}{N}\log \overline{S}_{\eta N} + o(1) \tag{24}$$

Define

$$E_1 \;\triangleq\; -\max_{\gamma \leq \eta \leq \epsilon}\left\{(1-\eta)h\left(\frac{\epsilon - \eta}{1 - \eta}\right) + \frac{1}{N}\log \overline{S}_{\eta N}\right\} \tag{25}$$

$$E_2 \;\triangleq\; -\max_{\substack{\gamma \leq \eta_2 \leq \eta_1 \leq \epsilon \\ 0 \leq \beta \leq \eta_2 \\ \eta_1 + \eta_2 - \beta \leq \epsilon}}\left\{(1 - (\eta_1 + \eta_2 - \beta))h\left(\frac{\epsilon - (\eta_1 + \eta_2 - \beta)}{1 - (\eta_1 + \eta_2 - \beta)}\right) + \frac{1}{N}\log \overline{S}_{\eta_1 N, \eta_2 N, \beta N}\right\} \tag{26}$$

then by combining (12), (13), (14), (21) and (24), we obtain that, w.p. at least $1 - \frac{\beta_{\eta,d,c}}{\epsilon^2} + o(1)$,

$$P_e^{\mathcal{C}}(\epsilon, N) \geq \frac{2}{r_\epsilon N + 1}2^{-N(E_1 + o(1))} - \frac{2}{r_\epsilon N(r_\epsilon N + 1)}2^{-N(E_2 + o(1))} \tag{27}$$

As we are interested in the asymptotic behavior of E_1 and E_2 (and thus the exponential growth rate of the stopping set distributions), we use [7, Theorem 2], which asserts the following[3]:

---

[3]Here we give the multivariate version of the theorem with 3 variables; the theorem generalizes to any number of variables.

Let $p(x, y, z)$ be a trivariate polynomial with non-negative coefficients. Let $\alpha_1 > 0, \alpha_2 > 0$ and $\alpha_3 > 0$ be some rational numbers and let n_i be the series of all indices such that

$$[x^{\alpha_1 n_i} y^{\alpha_2 n_i} z^{\alpha_3 n_i}] p(x, y, z)^{n_i} \neq 0$$

Then

$$\lim_{i \to \infty} \frac{1}{n_i} \log \left[x^{\alpha_1 n_i} y^{\alpha_2 n_i} z^{\alpha_3 n_i} \right] p(x, y, z)^{n_i} = \inf_{x>0, y>0, z>0} \log \left(\frac{p(x, y, z)}{x^{\alpha_1} y^{\alpha_2} x^{\alpha_3}} \right) \qquad (28)$$

Using (17), (18), (25), (26) and (28) we obtain

$$E_1 = -h(\epsilon) - \max_{\gamma \leq \eta \leq \epsilon} \left\{ \epsilon h \left(\frac{\eta}{\epsilon} \right) - ch(\eta) + \frac{c}{d} \inf_{x>0} \log \left(\frac{1 + \psi_2(x, d)}{x^{\eta d}} \right) \right\} \qquad (29)$$

$$E_2 = -h(\epsilon) - \max_{\substack{\gamma \leq \eta_1 \leq \eta_2 \leq \epsilon \\ 0 \leq \beta \leq \eta_2 \\ 0 \leq \eta_1 + \eta_2 - \beta \leq \epsilon}} \left\{ \epsilon h \left(\frac{\eta_1 - \beta}{\epsilon}, \frac{\eta_2 - \beta}{\epsilon}, \frac{\beta}{\epsilon} \right) - ch(\eta_1 - \beta, \eta_2 - \beta, \beta) \right.$$

$$\left. + \frac{c}{d} \inf_{x,y,z>0} \log \left(\frac{B(x, y, z, d)}{x^{(\eta_1 - \beta)d} y^{\beta d} z^{(\eta_2 - \beta)d}} \right) \right\}$$

If $E_2 \geq E_1$, we choose $r_{\epsilon N} = 1$ in (27). In this case, taking the union bound over all possible stopping sets yields an exponentially tight bound. In the case that $E_2 < E_1$, we use (27) with $r_{\epsilon N} = \lfloor 2^{N(E_1 - E_2 + \alpha)} \rfloor$, where $\alpha > 0$ can be made arbitrarily small (hence, the non-negativity of $\hat{P}_e^{\mathcal{C}}(\epsilon, N)$ in (11) is established). Thus, we obtain the following upper bound on the error exponent

$$-\frac{1}{N} \log P_e^{\mathcal{C}} < -\max_{\gamma \leq \epsilon \leq 1} \left\{ \epsilon \log \delta + (1 - \epsilon) \log(1 - \delta) - \left\{ \begin{array}{ll} E & \gamma \leq \epsilon \leq 1 - R \\ -h(\epsilon) & 1 - R \leq \epsilon \leq 1 \end{array} \right\} \right\} + o(1)$$

$$E \triangleq \left\{ \begin{array}{ll} E_1 & E_2 \geq E_1 \\ 2E_1 - E_2 & E_2 < E_1 \end{array} \right. \qquad (30)$$

This bound holds w.p. at least $1 - \frac{\beta_{\eta_0, d, c}}{\epsilon^2} + o(1)$, where η_0 is the maximizing value of η in (29).

IV. NUMERICAL RESULTS

In this section, we compare our upper bound on the error exponent of the BEC with previously-known lower bounds. These bounds were derived in [7, Theorems 8,12]; one of these bounds applies for iterative decoding, while the other applies for ML decoding.

In Figure 2 we exemplify our bound for the regular $(4, 8)$ LDPC ensemble. Recalling that the bound applies with a certain probability, we have marked the plot where the bound has a confidence level above 99%. We note that the entire plot of the upper bound is true w.p. at least 70%.

Figure 3 shows the confidence level bound from (23) which corresponds to the upper bound plot in Figure 2. Looking back at Figure 2 for low values of δ, the upper bound on the exponent coincides with the two lower bounds from [7, Theorems 6,8]. That is, our results indicate that in the region $\delta \in [0, 0.17]$, the bound on the error exponent of the expurgated ensemble in [7, Theorem 6], which coincides with the bound in [7, Theorem 8] in this region, is tight. Similarly, for the $(3, 6)$ ensemble and $\delta \in [0, 0.26]$,
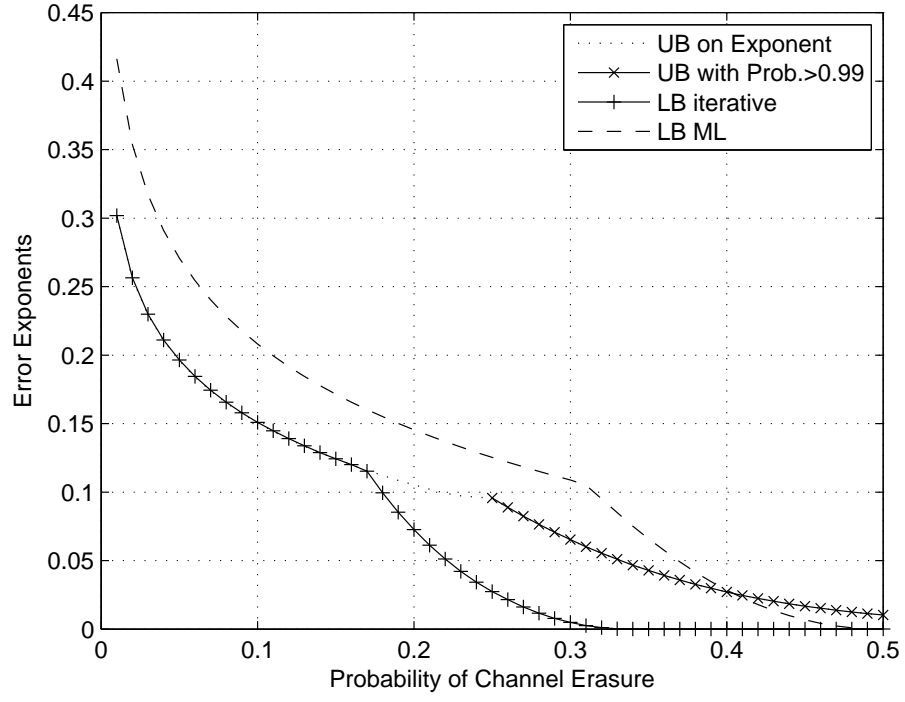
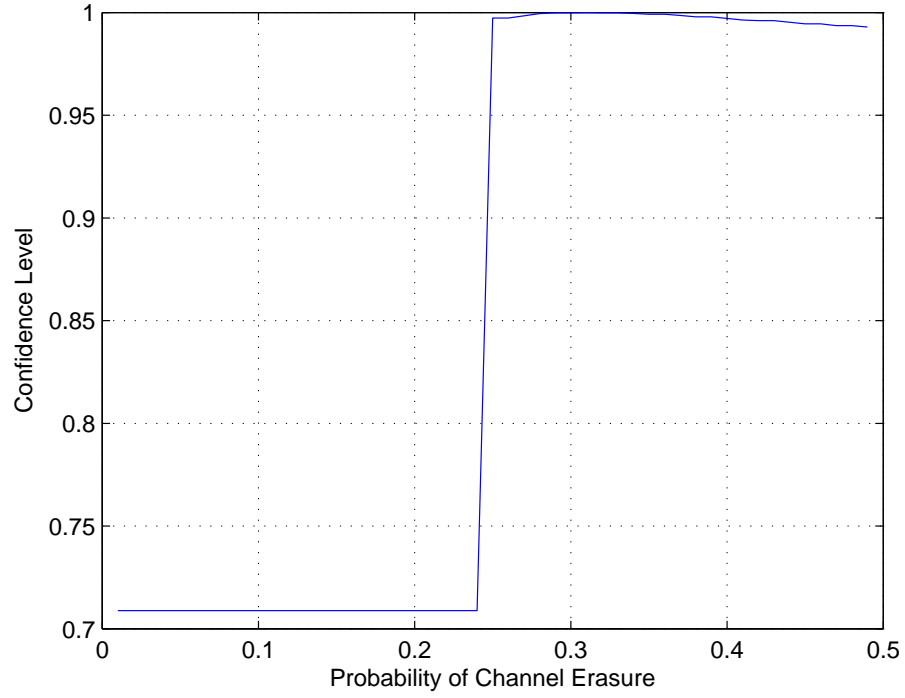Fig. 2.   Error exponents for the regular (4,8) LDPC ensemble.

Fig. 3.   Confidence level bound for the regular (4,8) LDPC ensemble.

the lower bound on the error exponent of the expurgated ensemble in [7, Theorems 6] (which coincides with the lower bound in [7, Theorem 8] in this region) is tight[4].

Focussing on higher values of δ where the confidence level is higher, comparison of our upper bound with the lower bound on the ML decoding exponent reveals that there is a gap in performance between iterative and ML decoders, at least for most codes in the ensemble.

V. CONCLUSION AND FURTHER RESEARCH

We have derived an upper bound on the error exponent of LDPC codes transmitted over the BEC. The upper bound relies on Dawson's inequality and holds with a certain confidence level. It was demonstrated that for some values of the channel erasure probability there is a gap between our upper bound and some previously reported lower bounds.

Continued research could focus on extending our results to irregular ensembles of LDPC codes. This requires to extend the results of [8], regarding concentration of stopping sets, to irregular codes. Another possible avenue is to try and bridge the gap between the lower and upper bounds; with the asymptotic decoding threshold for the $(4, 8)$ ensemble at about 0.38, there is still room for improvement in the bounds.

ACKNOWLEDGMENT

---

[4]We note that these lower bounds, as depicted in [7, Figure 3] do not coincide with each other in this δ region due to a numerical inaccuracy.

APPENDICES

APPENDIX I
PROOF OF (3)

Given the events $A_1, \ldots, A_M$ define the set B_s, $s = 1, \ldots, M$ as the set of points in $\bigcup_{i=1}^{M} A_i$ contained in exactly s sets. We thus have

$$\sum_{k=1}^{M} k\mathbf{1}_{\{B_k\}} = \sum_{k=1}^{M} \mathbf{1}_{\{A_k\}} = S_1 \tag{31}$$

$$\sum_{k=2}^{M} \binom{k}{2}\mathbf{1}_{\{B_k\}} = \sum_{k=1}^{M}\sum_{i=1}^{k-1} \mathbf{1}_{\{A_k\}}\mathbf{1}_{\{A_i\}} = S_2 \tag{32}$$

We will find a lower bound for

$$V = \mathbf{1}_{\{\bigcup_{i=1}^{M} A_i\}} = \sum_{k=1}^{M} \mathbf{1}_{\{B_k\}} \tag{33}$$

First, fix the value of r. Solving (31) and (32) to isolate $\mathbf{1}_{\{B_r\}}$ and $\mathbf{1}_{\{B_{r+1}\}}$ we get

$$\mathbf{1}_{\{B_r\}} = S_1 - \frac{2S_2}{r} - \mathbf{1}_{\{B_1\}} - \sum_{\substack{k=2 \\ k \neq r}}^{M} \mathbf{1}_{\{B_k\}}\frac{k(r+1-k)}{r} \tag{34}$$

$$\mathbf{1}_{\{B_{r+1}\}} = \mathbf{1}_{\{B_1\}}\frac{r-1}{r+1} + \frac{2S_2}{r+1} - S_1\frac{r-1}{r+1} - \sum_{\substack{k=2 \\ k \neq r+1}}^{M} \mathbf{1}_{\{B_k\}}\frac{k(k-r)}{r+1} \tag{35}$$

Substituting (34) and (35) into (33) we get

$$V - \frac{2S_1}{r+1} + \frac{2S_2}{r(r+1)} = \frac{r-1}{r+1}\mathbf{1}_{\{B_1\}} + \sum_{k=2}^{M} \mathbf{1}_{\{B_k\}}\frac{(r-k)(r-k+1)}{r(r+1)} \tag{36}$$

Note that the RHS of (36) contains only non-negative elements. Thus, if the RHS of (36) is replaced by zero, we obtain the inequality

$$V \geq \frac{2}{r+1}S_1 - \frac{2}{r(r+1)}S_2$$

which is the desired result.

APPENDIX II
CONFIDENCE INTERVAL OF STOPPING SET DISTRIBUTION

Rathi [8] has obtained a result asserting the concentration of the stopping set distribution. To state his result, we introduce some notation.

- Denote $\beta(x) \triangleq 1 + \psi_2(x, d)$, where ψ is defined in (15).
- The equation

$$x\frac{(1+x)^{d-1} - 1}{\beta(x)} = \eta$$

has a single real positive solution; denote this solution by x_η.

- Define $a_\beta(x) \triangleq \frac{x}{\beta(x)}\frac{d\beta(x)}{dx}$ and $b_\beta(x) \triangleq x\frac{da_\beta(x)}{dx}$
- Let $\underline{x} = (x_1, x_2, x_3)$. For a multivariate function $f(\underline{x})$, denote $a_f(\underline{x})$ to be a 3-element vector whose elements are $a_{f(i)} = \left(\frac{x_i}{f}\frac{\partial f}{\partial x_i}\right)$. Let $C_f(\underline{x})$ denote a 3×3 matrix whose elements are given by $C_{f(i,j)} = x_j\frac{\partial a_{f(i)}}{\partial x_j} = C_{f(j,i)}$.

The concentration result is as follows. The number of stopping sets $S_{\eta N}^{\mathcal{C}}$ in a randomly selected code $\mathcal{C}$ satisfies

$$\Pr\left(1 - \epsilon \leq \frac{S_{\eta N}^{\mathcal{C}}}{\bar{S}_{\eta N}} \leq 1 + \epsilon\right) \geq 1 - \frac{\beta_{\eta,d,c}}{\epsilon^2} + o(1) \tag{37}$$

where

$$
\begin{aligned}
\beta_{\eta,d,c} &= \frac{b_\beta(x_\eta)\sqrt{d}\eta(1-\eta)\sigma_c(\eta^2)}{\sqrt{|C_{\tilde{B}}(x_\eta, x_\eta^2, x_\eta)|(\eta^2(1-\eta)^2 - (c-1)\sigma_c^2(\eta^2))}} - 1 \\
\sigma_c^2(\eta^2) &= \frac{1}{cd|(-1,1,-1)\cdot C_{\tilde{B}}(x_\eta, x_\eta^2, x_\eta)^{-1}\cdot(-1,1,-1)^T|} \\
\tilde{B}(\underline{x}) &\triangleq B(x_1, x_2, x_3, d)
\end{aligned}
$$

and $B(\cdot, \cdot, \cdot, d)$ is defined in (19).

REFERENCES

[1] R. G. Gallager, *Low-Density Parity-Check Codes*, Cambridge, MA, USA, MIT Press, 1963.

[2] D.J.C. MacKay, "Good error-correcting codes based on very sparse matrices", *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 399–431, March 1999.

[3] A. Montanari, "The glassy phase of Gallager codes", *Europ. Phys. J.B.,*, vol. 23, pp. 121–136, 2001.

[4] D. Burshtein and G. Miller, "Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes", *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2696–2710, November 2001.

[5] O. Barak and D. Burshtein, "Lower Bounds on the Spectrum and Error Rate of LDPC Ensembles", *IEEE Transactions on Information Theory*, Vol. 53, no. 11, pp. 4225–4236, November 2007.

[6] S. Litsyn, V. Shevelev, "On Ensembles of Low-Density Parity-Check Codes: Asymptotic Distance Distributions", *IEEE Transactions on Information Theory*, vol. 48, no. 4, pp.887–908, April 2002.

[7] D. Burshtein and G. Miller, "Asymptotic enumeration methods for analyzing LDPC codes", *IEEE Transactions on Information Theory*, vol. 50, no. 6, pp. 1115–1131, June 2004.

[8] V. Rathi, "On the Asymptotic Weight and Stopping Set Distribution of Regular LDPC Ensembles", *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 4212–4218, September 2006.

[9] C. Di, T. Richardson, and R. Urbanke, "Weight Distribution of Low-Density Parity-Check Codes", *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 4839–4855, November 2006.

[10] A. Orlitsky, K. Viswanathan, J. Zhang, "Stopping Set Distribution of LDPC Code Ensembles", *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp.929–953, March 2005.

[11] M. Luby, M. Mitzenmacher, A. Shokrollahi and D. Spielman, "Improved low-density parity-check codes using irregular graphs", *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 585-598, February 2001.

[12] T. Richardson and R. Urbanke, "The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding", *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 599–618, February 2001.

[13] C. Di, D. Proietti, T. Richardson, E. Telatar, and R. Urbanke, "Finite Length Analysis of Low-Density Parity-Check Codes on the Binary Erasure Channel", *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp.1570–1579, June 2002.

[14] D.A. Dawson and D. Sankoff, "An inequality for probabilities", *Proc. Amer. Math. Soc.*, vol. 18, pp. 504–507, 1967.